



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/459,239	12/10/1999	HANID BACHA	CA9-98-030	9885

7590

04/29/2004

JAMES E NURRAY
69 SOUTH GATE DRIVE
POUGHKEEPIE, NY 12601

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/459,239

Applicant(s)

BACHA ET AL.

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 12-13, 22-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Carroll (US 6,105,131).

a. Referring to claim 1:

i. Carroll teaches:

(1) a data repository [i.e., as shown in Figure 1, a **secure server having data storage areas accessible through a standard secure web browser (column 1, lines 62-65)];**

(2) a repository manager for managing storage and retrieval of encrypted electronic data of a depositing computer into and out of the data repository [i.e., in Figure 2, a **vault deposit server comprises a connection secure server coupled to a vault process supervisor that manages access to vault processes (column 2, lines 6-8)];**

(3) an agent program of the depositing computer, accessible to the repository manager whether the depositing computer is online or off-line, the agent program having means in an environment secure from the repository manager to decrypt, on authentication of a requesting computer, the encrypted electronic data of the depositing computer retrieved from the data repository on request of the requesting computer [i.e., in Figure 2, the **vault process 50 runs in the vault deposit server on behalf of the owner of the vault where it resides. For example,**

a unique UNIX userid given sole access to a UNIX subdirectory, where the subdirectory is accessible only to an owner of the vault and has access privileges (which means no one could access but the owner of a personal vault – that is “in an environment secure from the repository manager”). In addition, vault processing decrypts the files using the vault encryption key (column 2, lines 9-14)].

b. Referring to claim 2 which depends on claim 1:

i. Carroll further teaches:

(1) where the repository manager is further adapted to digitally sign the encrypted electronic data prior to storage in the data repository, and to forward a copy of the signed encrypted data to the agent program of the depositing computer, and wherein the agent program of the depositing computer is adapted to verify in an environment secure from the repository manager against the signed encrypted data, the retrieved encrypted electronic data following decryption [i.e., In Figure 5, in step 80, if the user request access to a secure vault or process that resides on the secure server that issued the digital certificate, the user contacts the secure server and transmits the digital certificate to the secure server. In step 120, the vault deposit server evaluates the access request and digital certificate. In step 122, if the vault deposit server verifies the digital certificate, the user terminal is granted access to the secure vault containing the secure data or secure application, where the steps of retrieving data/application and decrypting information are inherently provided (column 9, lines 4-16)].

c. Referring to claim 3 which depends on claim 2:

i. Carroll further teaches:

(1) wherein the agent program is further adapted to forward the decrypted electronic data directly from the environment secure from the repository manager to the requesting computer without providing access to the repository manager [i.e., in Figure 5, personal vaults can be used for various purposes including but not limited to users vaults, validator vault, and certificate management system vaults. In step 86, if the request is verified, the validator

vault process transmits the request to the CMS for certification. After receiving the certificate from CMS, the validator vault process transmits the certificate to the user's browser (column 7, lines 39-40)].

d. Referring to claim 4 which depends on claim 3:

i. Carroll further teaches:

(1) wherein the agent program is a secure extension of the depositing computer and is adapted to manage communications between the depositing computer and the repository manager [i.e., in **Figure 2, the vault deposit server includes a connection secure server (a world wide web server that supports connections via SSL Ver. 3) coupled to a vault process supervisor which manages access to vault processes (column 5, lines 40-46)].**

e. Referring to claim 5 which depends on claim 4:

i. Carroll further teaches:

(1) a server having communication links with the repository manager, the depositing computer and the requesting computer [i.e., as **shown in Figure 1],**

(2) the server housing:

(a) the agent program of the depositing computer and the environment secure from the repository manager [i.e., **a vault process resides within the vault deposit server, whereby (column 5, line 44, see also Figure 2). In addition, the vault process 50 runs in the vault deposit server on behalf of the owner of the vault where it resides. For example, a unique UNIX userid given sole access to a UNIX subdirectory, where the subdirectory is accessible only to an owner of the vault and has access privileges (which means noone could access but the owner of a personal vault – that is “in an environment secure from the repository manager”) (column 2, lines 9-14)];**

(b) a second environment comprising a secure extension of the repository manager, said second environment adapted to manage communications to and from other environments on the server with the repository manager [i.e., in **Figure 2, a vault process supervisor is coupled to a vault process**

Art Unit: 2135

and a connection secure server (a world wide web server that supports connections via SSL Ver. 3, where the VPS manages access to vault processes (column 2, lines 7-8)); and

(c) at least a third environment comprising a secure extension of the requesting computer, said third environment adapted to manage communications to and from other environments on the server with the requesting computer [i.e., in Figure 1, a user terminal is coupled to a computer network through a secure server via a connection secure server (column 2, lines 49-52)].

f. Referring to claim 6 which depends on claim 5:

i. Carroll further teaches:

(1) wherein the agent program of the depositing computer comprises means to encrypt and digitally sign electronic data received from the depositing computer, and to forward the encrypted electronic data and signature to the repository manager for storage in the depositing computers data repository [i.e., the vault processes, execute on dedicated encrypted data in personal vault, are managed by the vault process supervisor. To execute a vault process, VPS must receive the vault certificate associated with the personal vault (column 5, lines 53-60). Protection of encrypted data transmitted from the vault process supervisor to personal vault includes encryption, digital signatures, and digital certificates (column 6, lines 6-7)].

g. Referring to claims 12 and 22:

i. Carroll teaches:

(1) digitally signing the electronic data at source [i.e., Protection of encrypted data transmitted from the vault process supervisor to personal vault includes encryption, digital signatures, and digital certificates (column 6, lines 6-7)];

(2) encrypting the electronic data at the source [i.e., user data stored in "personal vaults" managed by the server and encrypted by an encryption key (column 1, lines 60-61)];

Art Unit: 2135

(3) forwarding the encrypted electronic data to the data repository [i.e., in Figure 3A, a user terminal transmits a request to access a vault of application in a secure server (column 7, lines 35-37)];

(4) digitally signing the encrypted electronic data at the data repository to produce a deposit receipt [i.e., an approval or rejection notice is sent to the personal vault created for the user terminal (column 8, lines 26-28)];

(5) storing the encrypted electronic data and deposit receipt in the data repository in an environment free of access by the data repository manager [i.e., referring to Figure 1, Vault Depository Server 20, is for “storing the encrypted electronic data and deposit receipt in the data repository in an environment free of access by the data repository manager”]; and

(6) returning a copy of the deposit receipt to the source [i.e., referring to Figure 1, Secure Server 12, is for “returning a copy of the deposit receipt to the source” and the user terminal 18 can be “the source”].

h. Referring to claims 13 and 23:

i. Carroll further teaches:

(1) receiving a request from a requesting user, for access to the stored electronic data [i.e., the request is received at the registration authority terminal and is manually evaluated (column 8, lines 18-19)];

(2) retrieving the encrypted electronic data and forwarding the retrieved data to the source [i.e., the CMS transmits a new digital certificate to the user's personal vault. The vault process in the personal vault then transmits the new digital certificate to the user's browser (column 8, lines 38-41)];

(3) verifying the requesting user as authorized to access the electronic data [i.e., the CMS verifies the RA's approval notice and the public key (column 8, lines 37-38)]; and

(4) if verified, decrypting the retrieved data and sending it directly to the requesting user without providing access to the data repository manager

[i.e. vault processing decrypts the files using the vault encryption key(column 2, lines 13-14)].

3. Claims 7-8, 14-18, 25-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Chiu (US 6,181,336).

a. Referring to claims 7 and 17:

i. Chiu teaches:

(1) associating an access control list of user authorizations with the electronic data when stored in the data repository in an environment secure from the repository manager **[i.e., access control in the Vault repository is based on access control list (ACLs). An ACL identifies the users that are permitted access (which means only users and not system administrator) to the objects the ACL controls (column 24, lines 2-4). In addition, a user when creating a data object in the Vault repository 108 can override the system setting and restrict access to just himself if desired. This is useful for versions that represent work-in-progress and of which users are not ready to show to their colleagues (column 24 25-29)];**

(2) effecting updates to the access control list only from the source of the electronic data **[i.e., each repository has an ACL that controls who can change the ACLs of objects and version branches in the repository(column 24, lines 10-11). Individual users control when assets they are developing in their private workspaces, are to be made public and available to others, via the vault repository (column 16, lines 44-47)];**

(3) storing the updated access control list with the electronic data stored in the data repository in an environment secure from the repository manager; storing evidence of the updated access control list at the source of the electronic data and at any user computer to have effected the update **[i.e., the features provided by the vault API 106, as shown in Figure 1, include storage means storing both metadata and content data. As stated, information about assets, such as attributes, creator(s), storage location, date, etc., is referred to as the metadata component of the asset, and the contents of an asset itself is**

referred to as the content component of the asset (column 15, lines 50-55). In addition, a user when creating a data object in the Vault repository 108 can override the system setting and restrict access to just himself if desired. This is useful for versions that represent work-in-progress and of which users are not ready to show to their colleagues (column 24 25-29)]; and

(4) verifying accuracy of the updated access control list stored with the electronic data in the data repository with the evidence stored at the source before releasing the electronic data to a requesting authorized user [i.e., a user when creating a data object in the vault repository can override the system setting and restrict access to just himself if desired. This is useful for versions that represent work-in-progress and of which users are still reviewed/verified, and not ready to show to their colleagues (column 24, lines 25-29)].

b. Referring to claim 8 which depends on claim 7:

i. Chiu further teaches:

(1) the step of effecting updates to the access control list comprises:

(a) identifying a revision level of the updated access control list [i.e., each branch in a version tree has an ACL that determines who can create the next version in the branch (column 24, 8-9). Assets in the vault are immutable. That is, whenever a user modifies an asset and checks it back into the vault, a new version is automatically created (column 21, lines 15-20)]; and

(b) associating a current time stamp with the updated access control list [i.e., the features provided by the vault API 106, as shown in Figure 1, include storage means storing both metadata and content data. As stated, information about assets, such as attributes, creator(s), storage location, date, etc., is referred to as the metadata component of the asset (column 15, lines 50-55)], and

(2) the step of storing evidence comprises:

(a) creating a token of the revision level and current time stamp; and storing the token at every user with access to the electronic data in the data repository [i.e., **each asset includes two components, namely, a contents component and a metadata component. The metadata component comprises information about an asset, such as its storage location, creation date, creator(s), version, etc. Vault API stores both components in their repository (column 3, lines 11-15)]**].

c. Referring to claims 14, 15, 16, 24, 25, and 26:

i. These claims have limitations that is similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

d. Referring to claim 18 which depends on claim 17:

i. This claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 9-11, 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chiu, and further in view of Carroll.

a. Referring to claim 9 which depends on claim 8:

i. Chiu teaches:

(1) attaching the token to the updated access control list to form a data structure and storing the data structure with the updated access control list in the data repository and at the source [i.e., **attributes (its storage location, creation date, creator(s), version, etc. are stored in separate tables to facilitate**

efficient searching of assets stored within the vault repository (column 17, line 67 continue through column 18, line 1)];

ii. However, Chiu does not teach:

- (1) digitally signing the data structure and
- (2) verifying/decrypting the data structure signature at the

source; and

(3) comparing the verified data structure with the updated access control list retrieved from the data repository.

iii. Whereas, Carroll teaches:

(1) Protection of encrypted data transmitted from the vault process supervisor to personal vault includes encryption, digital signatures, and digital certificates **(column 6, lines 6-7);**

(2) vault processing decrypts the files using the vault encryption key **(column 2, lines 9-14);**

(3) the application server evaluates the request and digital certificate. The evaluation is an automated process to determine if the certificate is valid for the desired process and that the user is the owner of the digital certificate **(column 8, lines 63-67).**

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include digitally signatures and encryption/decryption (as shown in Figure 1 of Chiu) for further protection information storing in personal vault and/or vault repository against tampering by digital signatures and against untrusted communications with unknown parties by digital certificates **(column 2, lines 2-5 of Carroll).**

v. The ordinary skilled person would have been motivated to:

(1) add such feature as digital signatures and encryption/decryption (as shown in Figure 1 of Chiu) because an improved level of security and trust is needed for organizations to take advantage of distributed information networks in conducting business electrically, particularly in processing

sensitive customer information over the Internet or when processing transactions of significant financial or other fiduciary value (**column 1, lines 45-50 of Carroll**).

b. Referring to claim 10 which depends on claim 8:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

c. Referring to claim 11 which depends on claim 10:

i. Chiu further teaches:

(1) forwarding the digitally signed token to a user authorized by the source to update the access control list [**i.e., the Vault API permits an authorized person, for example, the production manager, to specify who has access to particular public assets and who may modify particular public assets (column 16, lines 41-44)**]; and

(2) on presentation of the digitally signed token by the user authorized to update the access control list [**i.e., with the ACL mechanism, an authorized user will be able to control the following types of accesses including: (1) who can create new versions of AMS data objects on a branch of an asset. Different access control may be applied to different branches of an asset; (2) who can read which data objects, and (3) who are authorized to make access control changes (column 24, lines 17-24)**].

ii. However, Chiu does not teach:

(1) verifying the token signature at the source; and

(2) comparing the verified token with the revision level and current time stamp associated with the updated access control list retrieved from the data repository.

iii. Whereas, Carroll teaches:

(1) the application server evaluates the request and digital certificate. The evaluation is an automated process to determine if the certificate is valid for the desired process and that the user is the owner of the digital certificate (**column 8, lines 63-67**).

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include digitally signatures and encryption/decryption (as shown in Figure 1 of Chiu) for further protection information storing in personal vault and/or vault repository against tampering by digital signatures and against untrusted communications with unknown parties by digital certificates (**column 2, lines 2-5 of Carroll**).

v. The ordinary skilled person would have been motivated to:

(1) add such feature as digital signatures and encryption/decryption (as shown in Figure 1 of Chiu) because an improved level of security and trust is needed for organizations to take advantage of distributed information networks in conducting business electrically, particularly in processing sensitive customer information over the Internet or when processing transactions of significant financial or other fiduciary value (**column 1, lines 45-50 of Carroll**).

d. Referring to claim 19 which depends on claim 18:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

e. Referring to claim 20 which depends on claim 18:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

f. Referring to claim 21 which depends on claim 20:

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

Response to Argument

6. Applicant's arguments filed February 17, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"The applicant's attorney did not find where the Carroll patent discloses preventing access by the repository administrator to either the vault owners vault or a directory of authorized users of data stored in the repository."

Examiner maintains that:

Carroll does teach the Personal vaults 40 assigned to users include logical collections of user data and user applications (vault processes) accessible only to authenticated users, which means if the repository administrator is not an authenticated user, the administrator cannot access to the personal vault (column 5, lines 44-47). Furthermore, the limitation, "in an environment secure from the repository manager", that the applicant added to the claims does not conform with the applicant's argument, "preventing access by the repository administrator".

Applicant further argues that:

"Applicant's attorney did not find where the Chiu patent teaches preventing access by the system administrator to a vault owners vault."

Examiner maintains that:

Chiu does disclose access control in the Vault repository 108 is based on access control lists (ACLs). An ACL identifies the users that are permitted access to the objects the ACL controls. When a user asks to access an object, his user id is checked against either the read, write or administrative ACL. The user is allowed access only if his user id is in the ACL (which means if a system administrator's id is not in ACL, the administrator cannot access the vault) (column 24, lines 1-7). In addition, a user when creating a data object in the Vault repository 108 can override the system setting and restrict access to just himself if desired. This is useful for versions that represent work-in-progress and of which users are not ready to show to their colleagues (column 24, lines 25-29).

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is

Art Unit: 2135

not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

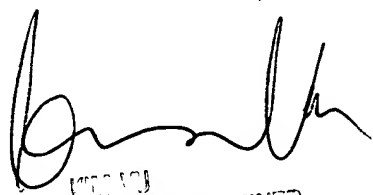
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

April 19, 2004



703-305-0327
SUPERVISOR / EXAMINER
TANYA TRUONG